EXHIBIT 3
DATE 2/3/09
HB 2

MONTANA OFFICE OF PUBLIC INSTRUCTION

STUDENT RECORDS CONFIDENTIALITY POLICY

Adopted February 1, 2008

Last Updated July 17, 2008

OPI
Linda McCulloch, Superintendent
Montana Office of Public Instruction
PO Box 202501
Helena, Montana 59620-2501
Toll Free: 1-888-231-9393, Local: 406-444-3095
www.opi.mt.gov

Montana Office of Public Instruction
Student Records Confidentiality Policy

Contents:

Student Records Confidentiality Policy
Montana Office of Public Instruction

I. PURPOSE

The purpose of this policy is to establish procedures and responsibilities governing the access, use and dissemination of confidential, sensitive and/or restricted student information by the Office of Public Instruction (OPI).

The collection of individual student information in AIM will replace previous collections of aggregated data from the following data systems:

- ADC (Annual Data Collection)
- MAEFAIRS (Montana Automated Education Finance and Information Reporting System)
- Carl Perkins Accountability
- Special Education Child Count

II. AUTHORIZATION

Individual student education records are submitted to the OPI for all students enrolled in K-12 public schools. The authority to require the submission of data is found in MCA 20-9-309 (2) (g) (See Exhibit 1). The initial appropriation for a K-12 Educational Data System was made in House Bill 2 from the 2005 legislative session. House Bill 2 (L. 2005) can be found at http://data.opi.mt.gov/bills/2005/billhtml/HB0002.htm.

The collection of student data will help facilitate the following:

- promote efficiencies (reduce reporting burden);
- build on existing technologies;
- provide a common basis of data reporting; and
- promote accountability needed to receive state funding.

III. SCOPE OF POLICY

These policies and procedures apply to all contractors and employees of the OPI and to all other entities requesting access to confidential, sensitive, or restricted student information.

Related policies, laws, operating procedures and other documents which contain directives that apply to agency confidential, sensitive and restricted enterprise information include:

- Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99 located at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html (See Exhibit 2.)
- State of Montana Policies located at http://itsd.mt.gov/policy/itpolicy.asp
    - ENT-SEC-041 Transmission Policy
    - ENT-SEC-130 Remote Access for Employees and Contractors
    - ENT-SEC-022 Network Server Security
    - ENT-INT-030 Internet Privacy and Security
    - ENT-SEC-081 User Responsibility
- Release of Information to the Public under the Public Information Act. MCA 2-6-102

- Montana School Accreditation Standards and Procedures Manual located at http://www.opi.mt.gov/pdf/accred/05accredmanual.pdf
- Destruction of Local Government Records, MCA 2-6-405 (d)
- Montana Secretary of State, Local Government Retention and Disposition Schedule located at http://sos.mt.gov/RMB/Local_Forms.asp#Local.
- OPI Records Management Policy
- Public Law 103-448, Section 9 and 108

IV. DEFINITIONS

Personally Identifiable Student Information
FERPA regulations defining *personally identifiable student information* include the following:

- The student's name;
- The name of the student's parent or other family member;
- The address of the student or student's family;
- A personal identifier such as social security number or student number;
- A list of personal characteristics that would make the student's identity easily traceable; or
- Other information that would make the student's identity easily traceable.

The above information cannot be disclosed without compliance with the requirements of FERPA.

Education Record
Education records are defined in FERPA as those records, files, documents, and other materials that contain information directly related to a student and are maintained by an education agency or institution or by a person acting for such agency or institution. 20 U.S.C. §1232g(a)(4). An education record is considered confidential because it contains personally identifiable information about a student.

All information submitted will be considered an education record and, therefore, is protected by Family Educational Rights and Privacy Act (FERPA, Exhibit 2). This federal law limits who can see an education record.

Student Records and Confidentiality Guidelines are outlined in Appendix C-1 of the Montana School Accreditation Standards and Procedures Manual located at http://www.opi.mt.gov/pdf/accred/05accredmanual.pdf.

Student Data Elements
Student data elements are individual pieces of data collected and stored by the OPI in a student's education record. The student data elements collected in the OPI's student information system are defined in the *AIM Data Dictionary* located at www.opi.mt.gov/pub/aim/DTA%20Dictionary.

Directory Information
FERPA allows school systems to establish a policy that designates some types of information as *directory information.* Directory information pertains to the portion of the education record that would not generally be considered harmful or an invasion of privacy if disclosed. Local education agency definitions of directory information may vary, but they generally include a student's name, address, and telephone number, and other

information typically found in school yearbooks or athletic programs. The FERPA regulations define *directory information* under § 99.3 of the regulations and set forth the requirements for implementing a directory information policy under § 99.37 of FERPA (Exhibit 2). Generally, *directory information* may be disclosed by a school to any party, provided the requirements of FERPA are followed. The OPI does not track the variation among local education agencies of their definitions of directory information. Additionally, the OPI is not informed which parents throughout Montana have refused to consent to disclosures of any personally identifiable information (some of which can be the same as directory information). Therefore, the OPI does not release directory information to any source.

Disclosure
Disclosure is to permit access to or the release, transfer, or other communication of education records, or the personally identifiable information contained in those records, to any party, by any means, including oral, written, or electronic means as defined in Appendix C of the Montana School Accreditation Standards and Procedures Manual.

V. STUDENT LOCATOR INFORMATION

Student-centered data collection systems such as AIM require the ability to assign a unique student identifier. An identifier is a computer-generated random number with no embedded meaning and is assigned to an individual student. This unique identifier is sometimes referred to as a "State ID." For the identifier to be unique, each student cannot have more than one identifier and each identifier cannot be associated with more than one student.

To ensure that each student has only one state identifier and that a single identifier is not assigned to more than one student, it is necessary for school personnel to review and locate whether a student has already been assigned a unique identifier before assigning a new identifier to any newly enrolled student. The process of reviewing and locating whether the student has already been assigned a unique identifier requires school personnel to access student locator information. Locator information includes:

- Student name
- Date of birth
- State ID
- Gender

The majority of locator information is confidential. Authorized school personnel have access to confidential locator information provided they have a reason for gaining access, such as the responsibility to assign unique student identifiers, or to determine if a student has already received a State ID, as may be the case when a student transfers from one school to another. All authorized school personnel who have access to confidential information must be familiar with policies and procedures to ensure confidentiality.

VI. PROGRAM PARTICIPATION INFORMATION

Program participation information identifies areas of program concentration and educational services provided to a student while enrolled in the school. Examples of the fields in this collection include students' status in relation to Title I, Free/Reduced Meal, LEP, Homeless, and Special Education. A complete list of fields can be found in the File Specifications document on the OPI AIM web site at http://www.opi.mt.gov/pub/AIM/File Specifications/. This information is part of the student's education record. Reporting of this information is subject to the OPI's policy for cell suppression.

VII. CELL SUPPRESSION POLICY

No cells of data that contain fewer than 10 students in a group will be publicly reported or released and must be suppressed to protect the identity of the student. The exceptions to this policy are enrollment, grade level, and gender, which are reportable down to one. The OPI will suppress data in the form of percentages when the percents are 0 or 100 for any student demographic categories with the exception of reports required under the State Accountability Workbook under NCLB. At the present time, this includes the following indicators: graduation, attendance, participation rates, and proficiency levels.

Any given numeric or non-numeric characteristic, variable values, or data element shared by fewer than 10 students in individual or aggregate (e.g., school, district, state) data sets or reports may contain potentially confidential student information. Even non-confidential student information may be confidential when combined with other data elements.

The OPI will report student counts to the U.S Department of Education and other federal agencies as required by federal laws and regulations governing education grant programs. The OPI will not suppress data reported to federal agencies. These federal agencies are subject to FERPA policy and regulations regarding the disclosure of confidential student information.

VIII. DISCLOSURE OF STUDENT INFORMATION

Part of the education record includes personal information about a student that can be made public according to this policy. The OPI may disclose, without consent, student information in aggregate form which is not easily traceable to a student. This information will follow the guidelines indicated in Section IX of this policy titled Obtaining Access to Student Information.

The OPI will disclose education records, without consent, to the parties listed immediately below under the following conditions:

- other schools when a student is transferring in order to facilitate school enrollment;
- specified officials for audit or evaluation purposes;
- organizations authorized by a school to conduct certain studies for or on behalf of the school; and
- appropriate officials in cases of health and safety emergencies.

The OPI recognizes school districts have developed their own policies to address FERPA (34 CFR § 99.31) compliance. In general, information about each request for records access and each disclosure of information

from an education record must be maintained as part of the record until the school or agency destroys the education record in accordance with the Montana Local Government Retention and Disposition Schedule, which can be found at http://sos.mt.gov/RMB/Local_Forms.asp#Local. The OPI AIM Records Retention Schedule can be found at http://www.opi.mt.gov/pub/AIM/AIM%20Policies.

IX. OBTAINING ACCESS TO STUDENT INFORMATION

This section describes the conditions under which the OPI will release confidential student information. Confidentiality refers to a person's obligation not to disclose or transmit information to unauthorized parties.

A. Access to Confidential Student Information

Access to confidential information carries with it the responsibility to protect the data. Access to confidential student information shall be granted only to personnel who are authorized by the OPI on a need-to-know basis in the performance of their duties.

An OPI Employee AIM and E-Grant Access Request Form (Exhibit 3) or an Affidavit of Non-Release of Data (Exhibit 4) must be signed by the requesting entity before any data will be released. Authorization must be evaluated annually to ensure access to the data is still required.

Intentional violations of this policy by an OPI employee may result in formal disciplinary action, up to and including termination, denial of access to sensitive data, and revocation of network access privileges.

Violation of this policy by agents of the OPI, other entities, or researchers inappropriately releasing data from an education record, whether through negligence or intent, will be subject to potentially permanent loss of access to education records. The OPI may utilize all legal remedies to recover any financial loss to the State which occurs due to negligent or intentional acts which constitute a violation of this policy. Any agents, other entities, or researchers who violate this policy, whether through negligence or intent, shall pay for the defense of all claims asserted against the State as a result of such violation.

The entities to which information may be released and the conditions of the release are listed for each entity below.

1) **OPI Staff** – The OPI staff who have a need to access confidential information in AIM must complete and submit an OPI Employee AIM Access Request Form (Exhibit 3) and the OPI Confidentiality Agreement (Exhibit 8) to the OPI Information Technology Services Division. The division administrator of the person requesting access to confidential information must sign the form which indicates the person needs access to this information in the performance of his or her assigned duties and responsibilities. The division administrator will ensure that the appropriate safeguards are instituted to protect the confidentiality of student information and that the staff person has received AIM training. The OPI staff may not access agency information for personal purposes (for example, research for a dissertation). Data will be destroyed in accordance with OPI's record retention policy.

Those staff who do not need access to AIM but who use confidential information concerning students or school districts in the course of their job duties must sign Exhibit 8 (OPI Confidentiality Agreement).

2) **Agent of the OPI** – An agent of the OPI is an entity that contracts with the OPI or with the U.S. Department of Education (DOE) and has written authorization from the DOE to analyze confidential data, or to provide some other service involving confidential data. When an agent contracts with another entity to provide a service involving confidential data, these entities are considered agents for data purposes. The OPI staff responsible for contracting with an entity to analyze confidential data or to provide some other service involving confidential data must ensure that the terms of the contract comply with the same conditions applicable to the OPI staff and that an Affidavit of Non-Release of Data (Exhibit 4) has been signed by the organization. A copy of the Affidavit of Non-Release of Data will be kept on file at the OPI, Information Technology Services Division. The agency staff person responsible for releasing the data must ensure that the Affidavit of Non-Release of Data has been signed prior to the data being released.

3) **Other Entities** – All other entities will be denied access to confidential information unless the entity is using the data to develop, validate, or administer predictive tests or improve instruction as defined in FERPA 34 C.F.R. § 99.31(a)(6). Authorized representatives of the Comptroller General of the United States, the Secretary of the U.S. Department of Education, or state and local educational authorities will be provided access to the data provided the disclosure is in the course of an audit, evaluation, compliance, or enforcement proceeding as defined in FERPA 34 C.F.R. §§ 99.31(a)(3), 99.35. The information will be protected to shield personal identification of students by others and the information will be destroyed when no longer needed.

4) **Researchers** - Researchers who are not an agent of the OPI or who are not employed or contracted by the agency or school may be authorized to conduct data processing or research and evaluation studies through contractual arrangements. Requests from researchers will be handled on a case-by-case basis after the request has been approved by the Data Privacy and Security Committee at the OPI. The Data Privacy and Security Committee members include the Measurement and Accountability Division Administrator, Chief of Staff, and Chief Legal Counsel at the OPI.

Items taken into consideration before releasing student data include:

- Perceived benefits of the research;
- Degree to which the research question cannot be answered without the confidential data;
- Potential invasion of student's privacy;
- Experience and reputation of the requester;
- Capacity of the requester to keep the data secure; and
- Availability of the OPI staff to fulfill the data request for the research project and monitor the process of the release and the research activities.

Such data will not be released unless the data are requested by an individual or organization who either (a) has developed a Research Proposal (Exhibit 6) which has been approved by the OPI Data Privacy and Security Committee and has completed the Research Project Confidentiality Agreement (Exhibit 7) or (b) has completed an Affidavit of Non-Release of Data (Exhibit 4). Once approval has been given to the researcher, the data will be posted to a secure file transfer protocol site which may then be downloaded.

In general, the release of data to researchers outside the agency is considered a loan of data (i.e., recipients do not have ownership of the data). Any personally identifiable student information shared with researchers must be destroyed when the data is no longer needed for the purposes for which it was requested.

Any requests for confidential student information from entities other than the OPI staff and its agents that do not meet the conditions of Section IX of this policy shall be directed to the district from which that information originated.

B. Procedures for Protecting Student Data

All agency employees, agents of the OPI, researchers, and other entities with direct access to confidential student information are responsible for protecting the data via the following procedures:

- Prevent disclosure of data by protecting visibility of reports and computer monitor when displaying confidential information.
- Workstations must be locked or shutdown when unattended.
- If reports containing any confidential student information are used in meetings or presentations, or presented to anyone without authorized access to the information, the agency employee or contractor must change the data to guarantee anonymity and omit or mask counts less than ten. One possible method for eliminating small counts is to reduce the number of variables used when selecting records (for example, by eliminating gender, the count may double).
- When no longer needed, paper reports must be shredded and electronic files must be destroyed in accordance with the Montana Secretary of State, Local Government Retention and Disposition Schedule.
- Confidential student information will not be faxed.
- Reports, CDs, and diskettes containing confidential student information must be stamped or otherwise marked as confidential prior to being released outside the agency. The envelope containing the information must also indicate that the contents are confidential.
- Confidential student information must be sent using encrypted email or by using the file transfer process set up in E-Pass. Instruction for using E-Pass can be found at http://opi.mt.gov/ITProjects/epass.html. Questions and concerns about transferring confidential data may be addressed to the OPI Network Services Bureau.

X. TRAINING NEEDS

All OPI staff and other entities requesting access to confidential student information shall be made aware of the AIM Student Records Confidentiality Policy and will receive subsequent information through newsletter articles, e-mail messages, and/or training classes.

XI. RESPONSIBILITY FOR PROCESS

The Information Technology Services and Measurement and Accountability Division at the OPI are primarily responsible for releasing AIM data once the appropriate form (Exhibit 3, 4, or 7) has been signed and approval has been granted by the Data Privacy and Security Committee.

The OPI Security Officer will file copies of all signed and approved file access request forms and confidentiality agreements (Exhibits 3, 4, 6, 7, 8) with the applicable data request. Any rights that need to be assigned to staff, agents of the OPI, or other entities will be assigned by the OPI Information Technology Services Division.

The OPI Measurement and Accountability Division staff are primarily responsible for releasing AIM data once the appropriate form (Exhibit 3, 4 or 7) has been signed and, for researchers, approval has been granted by the Data Privacy and Security Committee (Exhibit 6). The OPI Measurement and Accountability Division staff shall maintain a record which indicates the name of any individual or organization external to the OPI that requests data. The record of access shall also indicate the interest such individual or organization had in obtaining the information, the fields of data requested, and the date the requested data were disclosed. Once approval has been granted, the OPI Security Officer will process the security authorization and set up access to the records in compliance with FERPA guidelines.

XII. PROCESS FOR HANDLING INFORMATION REQUESTS FROM RESEARCHERS

Over the past several years, the OPI has received a growing number of information and data requests from researchers. Traditionally, these requests were handled on a case-by-case basis. However, as the number of such requests has grown, it has become necessary for the OPI to standardize the request approval process in order to handle these requests in a fair and timely manner. A description of the process follows.

A. External data requests for specific information will be honored only if one of the following is true:

1) The material requested has already been published or collected and can easily be put into a distribution format that protects confidential information. In these cases, information can be provided without a review by the OPI Data Privacy and Security Committee.

2) The requestor completes the process for conducting research with OPI data and has his/her proposal approved by the OPI Data Privacy and Security Committee. (See Exhibits 5 and 6.) Directions for an application to conduct research with student level data collected by the OPI are included in Exhibit 5.

B. Proposals submitted to the OPI Data Privacy and Security Committee will be subject to the following:

1) Before review by the OPI Data Privacy and Security Committee, proposals may be forwarded to appropriate staff within the OPI for their comments and recommendations. Information provided by the OPI staff will be considered in the proposal review.

2) Research proposals that fall under the OPI's primary mission statement will receive first priority.

3) The OPI staff resources may limit the number of requests that can be honored during a fiscal year. Thus, some worthy studies that receive approval may need to be postponed until OPI resources are available.

4) A charge may be associated with a data request/research proposal, including those approved by the OPI Data Privacy and Security Committee. The charge for already published documents will be determined by printing and mailing costs. The charge for conducting data selection/analysis tasks associated with a research proposal will vary but will not exceed $50 per hour. Cost estimates, if any, will be provided to the researcher upon request.

5) A conference will be held, by phone or in person, with researchers whose proposals have been accepted. During the conference, members of the OPI Data Privacy and Security Committee and the researcher(s) will come to an agreement on objectives, end products, timelines, areas of responsibility, data security arrangements, authorship credit, and costs. A written statement outlining the terms of the agreement will be signed by the researcher and a designee of the OPI Data Privacy and Security Committee.

6) A Research Project Confidentiality Agreement must be signed by each researcher once the OPI Data Privacy and Security Committee approves the research request for data. (See Exhibit 7.)

7) The OPI Data Privacy and Security Committee will meet as needed to consider proposals.

8) Researchers will provide a copy of products resulting from the research (e.g., publication, report, book) to the OPI Data Privacy and Security Committee.

C. Documentation of all research requests will be maintained.

1) The OPI staff will track each research project and data request.

2) Files sent and technical assistance given to researchers will be included in the data request tracking documentation.

3) The OPI staff will attach a copy of the end result of a research project (publication, report, book) or a link to the material to the data request tracking documentation.

XIII. ENFORCEMENT

The Family Policy Compliance Office of the U.S. Department of Education is responsible for enforcement regarding concerns of breach of confidentiality or violations of FERPA and can be reached by calling (202) 260-3887 or at the following address:
US Department of Education
600 Independent Avenue, SW
Washington, DC 20202-4605

XIV. EXHIBIT 1
Statutory Authorization to Collect Student Data

The authority to require the submission of data is found in MCA 20-9-309 (2) (g). The initial appropriation for a K-12 Educational Data System was made in House Bill 2 from the 2005 legislative session. The complete text of House Bill 2 can be found at http://data.opi.mt.gov/bills/2005/billhtml/HB0002.htm.

MCA 20-9-309. Basic system of free quality public elementary and secondary schools defined -- identifying educationally relevant factors -- establishment of funding formula and budgetary structure -- legislative review. (1) Pursuant to Article X, section 1, of the Montana constitution, the legislature is required to provide a basic system of free quality public elementary and secondary schools throughout the state of Montana that will guarantee equality of educational opportunity to all.

(2) As used in this section, a "basic system of free quality public elementary and secondary schools" means:

(a) the educational program specified by the accreditation standards provided for in 20-7-111, which represent the minimum standards upon which a basic system of free quality public elementary and secondary schools is built;

(b) educational programs to provide for students with special needs, such as:

(i) a child with a disability, as defined in 20-7-401;

(ii) an at-risk student;

(iii) a student with limited English proficiency;

(iv) a child who is qualified for services under 29 U.S.C. 794; and

(v) gifted and talented children, as defined in 20-7-901;

(c) educational programs to implement the provisions of Article X, section 1(2), of the Montana constitution and Title 20, chapter 1, part 5, through development of curricula designed to integrate the distinct and unique cultural heritage of American Indians into the curricula, with particular emphasis on Montana Indians;

(d) qualified and effective teachers or administrators and qualified staff to implement the programs in subsections (2)(a) through (2)(c);

(e) facilities and distance learning technologies associated with meeting the accreditation standards;

(f) transportation of students pursuant to Title 20, chapter 10;

(g) *a procedure to assess and track student achievement in the programs established pursuant to subsections (2)(a) through (2)(c)*; and

(h) preservation of local control of schools in each district vested in a board of trustees pursuant to Article X, section 8, of the Montana constitution.

(3) In developing a mechanism to fund the basic system of free quality public elementary and secondary schools and in making adjustments to the funding formula, the legislature shall, at a minimum, consider the following educationally relevant factors:

(a) the number of students in a district;

(b) the needs of isolated schools with low population density;

(c) the needs of urban schools with high population density;

(d) the needs of students with special needs, such as a child with a disability, an at-risk student, a student with limited English proficiency, a child who is qualified for services under 29 U.S.C. 794, and gifted and talented children;

(e) the needs of American Indian students; and

(f) the ability of school districts to attract and retain qualified educators and other personnel.

(4) By July 1, 2007, the legislature shall:

(a) determine the costs of providing the basic system of free quality public elementary and secondary

schools;

(b) establish a funding formula that:

(i) is based on the definition of a basic system of free quality public elementary and secondary schools and reflects the costs associated with providing that system as determined in subsection (4)(a);

(ii) allows the legislature to adjust the funding formula based on the educationally relevant factors identified in this section;

(iii) is self-executing and includes a mechanism for annual inflationary adjustments;

(iv) is based on state laws;

(v) is based on federal education laws consistent with Montana's constitution and laws; and

(vi) distributes to school districts in an equitable manner the state's share of the costs of the basic system of free quality public elementary and secondary schools; and

(c) consolidate the budgetary fund structure to create the number and types of funds necessary to provide school districts with the greatest budgetary flexibility while ensuring accountability and efficiency.

(5) At least every 10 years following April 7, 2005, the legislature shall:

(a) authorize a study to reassess the educational needs and costs related to the basic system of free quality public elementary and secondary schools; and

(b) if necessary, incorporate the results of those assessments into the state's funding formula.

History: En. Sec. 2, Ch. 208, L. 2005.

XV. EXHIBIT 2
An Overview of the Family Educational Rights and Privacy Act (FERPA)

Student education records are official and confidential documents protected by one of the nation's strongest privacy protection laws, the Family Educational Rights and Privacy Act (FERPA). FERPA, also known as the Buckley Amendment, defines education records as all records that schools or education agencies maintain about students.

FERPA gives parents (as well as students in postsecondary schools) the right to review and confirm the accuracy of education records. This and other United States "privacy" laws ensure that information about citizens collected by schools and government agencies can be released only for specific and legally defined purposes. Since enacting FERPA in 1974, Congress has strengthened privacy safeguards of education records through this law, refining and clarifying family rights and agency responsibilities to protect those rights.

FERPA's legal statute citation can be found in the U.S. Code (20 USC 1232g), which incorporates all amendments to FERPA. FERPA regulations are found in the Federal Register (34 CFR Part 99). FERPA's 1994 amendments are found in Public Law (P.L.) 103-382.

FERPA Protects Privacy

FERPA applies to public schools and state or local education agencies that receive Federal education funds, and it protects both paper and computerized records. In addition to the Federal laws that restrict disclosure of information from student records, most states also have privacy protection laws that reinforce FERPA. State laws can supplement FERPA, but compliance with FERPA is necessary if schools are to continue to be eligible to receive Federal education funds.

FERPA requires schools and local education agencies to annually notify parents of their rights under FERPA. The notice must effectively inform parents with disabilities or who have a primary home language other than English. The annual notice pertaining to FERPA rights must explain that parents may inspect and review records and, if they believe the records to be inaccurate, they may seek to amend them. Parents also have the right to consent to disclosures of personally identifiable information in the record, except under authorized circumstances.

FERPA gives both parents, custodial and non-custodial, equal access to student information unless the school has evidence of a court order or state law revoking these rights. When students reach the age of 18, or when they become students at postsecondary education institutions, they become "eligible students' and rights under FERPA transfer to them. However, parents retain access to student records of children who are their dependents for tax purposes.

FERPA Defines an Education Record

Education records include a range of information about a student that is maintained in schools in any recorded way, such as handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. Examples are:

- *Date and place of birth, parent(s) and/or guardian addresses, and where parents can be contacted in emergencies;*
- *Grades, test scores, courses taken, academic specializations and activities, and official letters regarding a student's status in school;*
- *Special education records;*
- *Disciplinary records;*
- *Medical and health records, including immunization records, that the school creates or collects and maintains;*
- *Documentation of attendance, schools attended, courses taken, awards conferred, and degrees earned;*
- *Personal information such as student's identification code, social security number, picture, or other information that would make it easy to identify or locate a student.*

Personal notes made by teachers and other school officials that are not shared with others are not considered education records. Additionally, law enforcement records created and maintained by a school or district's law enforcement unit are not education records.

Part of the education record, known as ***directory information***, includes personal information about a student that can be made public according to a school system's student records policy. Directory information may include a student's name, address, and telephone number, and other information typically found in school yearbooks or athletic programs. Other examples are names and pictures of participants in various extracurricular activities or recipients of awards, pictures of students, and height and weight of athletes.

Each year schools must give parents public notice of the types of information designated as directory information. By a specified time after parents are notified of their review rights, parents may ask to remove all or part of the information on their child that they do not wish to be available to the public without their consent.

FERPA Guarantees Parent Review and Appeal

If, upon review, parents find an education record is inaccurate or misleading, they may request changes or corrections, and schools and education agencies must respond promptly to these requests.

Requests should be made in writing, according to an agency's annual notice of procedures for exercising rights to amend records. Within a reasonable time period, the school or agency must decide if the request to change a record is consistent with its own assessment of the accuracy of the record. If a parent's request is denied, he or she must be offered the opportunity for a hearing. If the disagreement with the record continues after the hearing, the parent may insert an explanation of the objection in the record. FERPA's provisions do not apply to grades and educational decisions about children that school personnel make.

While parents have a right to review records, schools are not required by Federal law to provide copies of information, unless providing copies would be the only way of giving parents access. Schools may charge a reasonable fee for obtaining records, and they may not destroy records if a request for access is pending.

FERPA Restricts Disclosure of Student Records

Local education agencies and schools may release information from students' education records with the prior written consent of parents, under limited conditions specified by law, or as stated in local agencies' student records policies. The same rules restricting disclosures apply to records maintained by third parties acting on behalf of schools, such as state and local education agencies, intermediate administrative units, researchers, psychologists, or medical practitioners who work for or are under contract to schools.

If an agency or school district has a policy of disclosing records, it must specify the criteria for determining school officials within an agency, including teachers, who have a legitimate educational interest. Generally, school officials have legitimate educational interest if they need to review an education record to fulfill their professional responsibilities.

Teachers and school officials who work with the students and schools to which students apply for entrance may also have access to education records without prior consent of the parent. In addition, information from students' records may be released to state and local education officials to conduct audits or to review records in compliance with Federal laws. Schools may also disclose information from education records without the consent of parents in response to subpoenas or court orders. A school official must make a reasonable effort to notify the parent before complying with the subpoena unless the subpoena is issued to enforce a law and specifies not to notify the parent. In emergencies, school officials can provide information from education records to protect the health or safety of the student or others.

There are cases when schools or school systems decide it is in the public interests to participate in policy evaluations or research studies. If student records are to be released for these purposes, the school or school system must obtain prior consent of the parent. Signed and dated written consent must:

- *Specify the records that will be released;*
- *State the reason for releasing the records;*
- *Identify the groups or individuals who will receive the records.*

In general, information about each request for records access and each disclosure of information from an education record must be maintained as part of the record until the school or agency destroys the education record. Outside parties receiving records must receive a written explanation of the restrictions on the re-release of information.

Additional FERPA Provisions

In 1994, the Improving America's School Act amended several components of FERPA, tightening privacy assurances for students and families. The amendments apply to the following key areas:

- *Parents have the right to review the education records of their children maintained by the state education agencies;*
- *Any third party that inappropriately re-releases personally identifiable information from an education record cannot have access to education records for five years;*
- *Information about disciplinary actions taken against students may be shared, without prior consent of the parent, with officials in other education institutions;*
- *Schools may release records in compliance with certain law enforcement judicial orders and subpoenas without notifying parents.*

Questions? Call the Local School System, State Education Agency, or the Federal Family Policy Compliance Office.

School districts, state education agencies, and the U.S. Department of Education all offer assistance about FERPA. Before contacting Federal officials, however, you can often get a direct and immediate response from your local or state education officials.

The **Family Policy Compliance Office** can be reached at the following address;

U.S. Department of Education
600 Independent Avenue, SW
Washington, DC 20202-4605
(202) 260-3887

XVI. EXHIBIT 3

OPI Employee AIM Access Request

This form will be used to identify each individual who will use AIM. . The completed form is to be sent to the OPI Help Desk who will set up the user security roles. If you have questions regarding this form, please contact the OPI Help Desk at 444-3448.

Name of Individual Requesting Access: *(Please Print)* _____

Division: _____ Bureau: _____

Briefly describe your primary use of the AIM system: _____

_____

_____

TYPE OF ACCESS REQUESTED:

- ☐ **Read** - Read-only rights to specific student information (census, enrollment, & state reporting tools). Rights to view calendars. No read rights to specific special education information or database/system administrator tools.
- ☐ **Read All** - Read-only rights to all student information (census, enrollment & state reporting tools); including read only rights to special education data. Rights to all view calendars.
- ☐ **Ad Hoc Reporting** – Allows user to create, edit, and delete filters. Rights to export data for reports. Rights to create, modify and save a cube.
- ☐ **District Assistance RW**- Allows user to modify specific student information (census, enrollment & state reporting data elements) to assist districts with their data entry and clean up. Rights to all calendars. Rights to view special education status. No rights to view special education data (forms, IEP). No rights to update directory information.
- ☐ **District Assistance RWAD**- Allows user to enter, modify, and delete a student record (census, enrollment & state reporting data elements) to assist districts with their data entry and clean up. Rights to all calendars and all student information (excluding special education data). No rights to update or view special education data. No rights to update directory information.
- ☐ **Directory R** – Allows user to view school and district directory information (System Admin>Resources).
- ☐ **Directory RWA**- Allows user to view, modify and add school and district directory information (System Admin>Resources).
- ☐ **Combine/Delete Records** - Rights to combine duplicate student records and delete enrollments student records. No rights to update directory information.
- ☐ **Migrant** – Allows user to modify student enrollment data, specifically migrant information.
- ☐ **Special Education Read** - Read rights all student information including special education specific data (summary, team members, documents, contact log). Rights to all calendars.
- ☐ **Special Education Monitors RW**– Allows user to modify (or write) specific areas of the Special Education documents including IEP.
- ☐ Other (Describe specific duties): _____

_____

CONFIDENTIALITY/CONSENT STATEMENT: *(To be read and signed by the individual requiring access.)*
I hereby certify that I am entitled to the confidential information to which I am requesting access. I will not release the confidential information to others unless it is for purposes directly connected to the administration of the program for whose purposes it was originally provided. Intentional violations of the OPI Student Records Confidentiality Policy may result in formal disciplinary action, up to and including termination, denial of access to sensitive data, and revocation of network access privileges. I have read and signed the OPI Network Acceptable Use Policy, the OPI Student Records Confidentiality Policy, and the State of Montana's Computer Use Policies and I agree to comply with all terms and conditions.

Employee Signature: _____ Date: _____

Division Administrator Signature: _____ Date: _____

This section to be completed by the OPI security officer

Signature of Security Officer: _____ Date: _____

Access Approved: ☐ Access Denied: ☐ Logon ID: _____

XVII. EXHIBIT 4
Affidavit of Non-Release of Data for Agents of OPI or Other Entities

This form will be used to identify an agent of OPI or other entity who requests access to confidential student information. The completed form is to be sent to the OPI Help Desk who will forward it to the OPI Data Privacy and Security Committee for review and approval. Once approved, the OPI Help Desk will set up the user security roles. If you have questions regarding this form, please contact the OPI Help Desk at 444-3448.

I, _____, do solemnly swear that when given access to the student information data provided by the OPI, I shall only 1) use, reveal, or in any other manner disclose any personally identifiable information furnished, acquired, retrieved, or assembled by me or others, or 2) make any release or publication by which an individual could be identified to authorized staff at the OPI and authorized school district representatives in order to: (check all that apply)

☐ Audit or evaluate ☐ Comply with an enforcement proceeding

☐ Improve instruction ☐ Develop, validate, or administer predictive tests

☐ Provide training and system support

☐ Other (please describe) _____

I shall not permit anyone other than the individuals authorized by _____ (name of the agency or school) to examine the individual records.

The re-release of such student information in any other circumstances is prohibited by the Family Educational Rights and Privacy Act of 1974.

Please provide a detailed description of how the data will be kept secure, including computer security, physical handling, and storage and transportation of data.

_____

I understand if, through my negligent or intentional acts, I violate this policy by inappropriately releasing data from an education record, I will be subject to potentially permanent loss of access to education records. Additionally, I understand and agree the OPI may utilize all legal remedies to recover for any financial loss to the State which occurs due to my negligent or intentional acts which constitute a violation of this policy. I further agree to pay for the defense of all claims asserted against the State as a result of my negligent or intentional acts which constitute a violation of this policy.

Signature: _____

Name: _____ Title: _____

Organization: _____ Date: _____

Notary Public and Seal: _____

This section to be completed by the OPI staff:
LOA or Contract #

Access Approved ☐ _____ **Access Denied** ☐ _____
Effective Dates of Contract: _____

Signature of Security Officer: **Date:**

XIX. EXHIBIT 5
Directions for Application to Conduct Research with Student Level Data Collected by the OPI

Student level data will be released to researchers who complete the Research Proposal Application (Exhibit 6) after the proposal has been approved by the OPI Data Privacy and Security Committee and the Research Project Confidentiality Agreement (Exhibit 7) has been signed by the responsible parties. Researchers who are interested in such an arrangement should comply with the following directions. Those agencies under contract with the OPI must complete and sign the Affidavit of Non-Release of Data for Agents of the OPI or Other Entities (Exhibit 4).

1. Researcher must complete the Research Proposal Application (Exhibit 6) and submit the form to the OPI Measurement and Accountability Division, Office of Public Instruction, PO Box 202501, Helena, Montana 59620-2501.

2. Research proposals received will be reviewed by the OPI Data Privacy and Security Committee. As necessary, the OPI legal staff and program staff from the department most closely connected to the research topic may be included in the review process. Researchers will be informed of the committee's decision about acceptance/rejection of the proposal in as timely a manner as possible.

3. Either at the time of the submission of the documents referred to in item 1, or upon having a research project accepted, the researcher must complete the Research Project Confidentiality Agreement (Exhibit 7) and send it to the OPI Measurement and Accountability Division.

4. Once a proposal is accepted, researchers and the appointed OPI liaison will confer for the purpose of developing an agreement related to objectives, end products, timelines, areas of responsibility, data security arrangements, authorship credit, and costs. This agreement must be signed by the Researcher and approved by the OPI liaison.

5. Once an agreement has been signed, access to data will be granted.

6. Questions about directions or procedures for research may be addressed to the Office of Public Instruction, Measurement and Accountability Division.

XVIII. EXHIBIT 6
Research Proposal Application

This form will be used to identify the researcher who requests access to confidential student information. The completed form should be submitted to the OPI Data Privacy and Security Committee, Office of Public Instruction, PO Box 20501, Helena, MT 59620-2501.

Title of Proposed Research Project:	
Research Individual or Organization Name:	
Address:	
Name of Primary Researcher:	
Title:	
Phone:	Email:

Provide a description of the research to be performed, including the following:

1) the research question(s) to be addressed;
2) potential improvements or benefits to Montana education of answering the questions;
3) the organization sponsoring the research;
4) research timeline;
5) the specific data items that will be requested from the Montana Office of Public Instruction (OPI);
6) other data that will be collected for the research and from whom;
7) how the data will be used and analyzed;[1]
8) how the analysis will be reported and to whom;
9) the names and titles of the professional and support staff who will conduct the research and analysis;[2]
10) the estimated time the data from the OPI will be needed; and
11) a detailed description of how the data will be kept secure, including computer security, physical handling and storage of data, and transportation of data.

This section to be completed by the OPI Data Privacy and Security Committee
Signature: _____ Date: _____

Access Approved: ☐ Access Denied: ☐

[1] Data must only be used for purposes associated with the data collection and analysis specified in this Research Proposal.
[2] Attach research staff VITA.

XX. EXHIBIT 7
Research Project Confidentiality Agreement

The Montana Office of Public Instruction (OPI) has collected certain data that contain confidential personally-identifiable information; the OPI requires this confidentiality to be protected.

The OPI is willing to make these data available for research and analysis purposes to improve instruction in public elementary and secondary schools, but only if the data are used and protected in accordance with the terms and conditions stated in this Agreement.

(Insert typed name and address of Research Organization) (Researcher) and the OPI agree as follows:

I. INFORMATION SUBJECT TO THIS AGREEMENT

A. All data containing personally-identifiable information collected by or on behalf of the OPI and provided to the Researcher and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by the OPI with other data, are subject to this Agreement and are referred to herein as the "subject data." The subject data under this Agreement may be stated or provided in various forms, including, but not limited, to written or printed documents, computer tapes, diskettes, CD-ROMs, hard copy, or encrypted files.

B. The Researcher may use the subject data only for the purposes stated in the Research Proposal Application attached hereto and made a part of this Agreement (marked as Attachment 1), and is subject to the limitations imposed under the provisions of this Agreement.

II. INDIVIDUALS WHO MAY HAVE ACCESS TO SUBJECT DATA

Researcher agrees to limit and restrict access to the subject data to the following three categories of individuals:

1. The Project Leaders who are in charge of the day-to-day operations of the research and who are the research liaisons with the OPI.

2. The Professional/Technical staff in charge of the research under this Agreement.

3. Support staff including secretaries, typists, computer technicians, etc.; however, these individuals shall be allowed access to the subject data only to the extent necessary to support the research.

III. LIMITATIONS ON DISCLOSURE

A. Researcher shall not use or disclose the subject data for any purpose not expressly stated in the Research Proposal Application approved by the OPI unless the Researcher has obtained advance written approval from the OPI.

B. Researcher may publish the results, analysis, or other information developed as a result of any research based on the subject data made available under this Agreement only in summary or aggregate form, ensuring the identities of individuals included in the subject data are not revealed.

IV. ADMINISTRATIVE REQUIREMENTS

A. The research conducted under this Agreement shall be limited to, and consistent with, the purposes stated in the Research Proposal Application.

B. Notice and training on confidentiality and nondisclosure.

1. Researcher shall notify and train each of its employees who will have access to the subject data of the strict confidentiality of such data, and shall require each of those employees to execute an Affidavit of Non-Release of Data for Agents of OPI, Other Entities or Researchers.

2. Researcher shall maintain each executed Affidavit of Non-Release of Data for Agents of OPI, Other Entities or Researchers at its facility, and shall allow inspection of the same by the OPI upon request.

3. Researcher shall promptly notify the OPI in writing when the access to the subject data by any individual is terminated, giving the name of the individual and the date of the termination.

C. Publications made available to the OPI.

1. Researcher shall provide the OPI a copy of each publication containing information based on the subject data or other data product based on the subject data made available through the OPI.

D. Researcher shall notify the OPI immediately in writing upon receipt of any request or demand for disclosure of the subject data.

E. Researcher shall notify the OPI immediately in writing upon discovering any breach, or suspected breach, of security, or of any disclosure of subject data to an unauthorized party or agency.

V. SECURITY REQUIREMENTS

A. Maintenance of, and access to, the subject data.

1. Researcher shall retain the original version of the subject data at a single location and shall not make a copy or extract of the subject data available to anyone except individuals specified in paragraph II.

2. Researcher shall maintain the subject data (whether maintained on a mainframe facility, central server, personal computer, or in print or other medium materials) in an area with access limited to only authorized personnel. Researcher shall not permit removal of any subject data from the limited access area.

3. Researcher shall ensure access to the subject data maintained in computer files or databases is controlled by password protection. Researcher shall maintain all printouts, diskettes, or other physical products containing individually-identifiable information derived from subject data in locked cabinets, file drawers, or other secure locations when not in use.

4. Researcher shall ensure all printouts, tabulations, and reports are edited to prevent any possible disclosure of personally-identifiable subject data.

5. Researcher shall establish procedures to ensure the subject data cannot be extracted from a computer file or database by unauthorized individuals.

B. Retention of subject data.

1. Researcher shall destroy the subject data, including all copies, when the research that is the subject of this Agreement has been completed or this Agreement terminates, whichever occurs first.

VI. TERMINATION OF THIS AGREEMENT

1. This Agreement shall terminate six months from the date it is signed by the OPI. The Agreement, however, may be extended by written agreement of both of the parties.

2. Any violation of the terms and conditions of this Agreement may result in the immediate revocation of this Agreement by the OPI.

   a. The OPI may initiate revocation of this Agreement by written notice to Researcher indicating the factual basis and grounds of revocation.
   b. Upon receipt of the written notice of revocation, the Researcher shall immediately cease all research activity related to the Agreement until the issue is resolved. The Researcher will have three business days to submit a written Response to the OPI indicating why this Agreement should not be revoked.
   c. The OPI Data Privacy and Security Committee shall decide whether to revoke this Agreement based on all the information available to it. The OPI shall provide written notice of its decision to the Researcher within 10 business days after receipt of the Response. These timeframes may extend for good cause.

SIGNATURE PAGE

By signing below, the individual researcher or official of the Research Organization certifies he or she has the authority to bind the Research Organization to the terms of this Agreement and that the Research Organization has the capability to undertake the commitments in this Agreement.

1. Location at which the subject data will be maintained and analyzed.	
2. Signature of the Individual Researcher or Official of the Research Organization	3. Date
4. Type/Print Name of Official	5. E-mail
6. Title	7. Telephone
8. Mailing Address	
9. Signature of the Principal Research Analyst	10. Date
11. Type/Print Name of Principal Research Analyst	12. E-mail
13. Title	14. Telephone
15. Mailing Address	
16. Signature of OPI Research Liaison	17. Date
18. Type/Print Name of OPI Research Liaison	19. E-mail
20. Title	21. Telephone
22. Mailing Address	

XXI. EXHIBIT 8
OPI Confidentiality Agreement

As an employee of the Montana Office of Public Instruction (OPI) you may often come in contact with confidential information concerning students and school districts. Employees are required to maintain confidentiality in all areas and may include written or computerized district data, other written material or verbal conversations.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

FERPA information must be kept confidential.

The OPI is committed to complying with FERPA and other State and Federal laws protecting our districts' privacy.

Violation of the provisions of FERPA can result in civil and criminal penalties for OPI and disciplinary action against the employee, up to and including termination.

Guidelines for maintaining confidentiality:

1. Access only those records you need to perform your duties or as authorized by your supervisor.
2. Provide confidential information only to those persons who are authorized to receive it. Your supervisor can give you direction if you are unsure about who has access to the information.
3. Report any suspected breach of confidentiality to your supervisor as you become aware of it.

OPI Employees must make reasonable efforts to provide for the security of confidential information.

1. Security of electronic information
   a. Employees will be granted access to only the level of information that is required by their job duties.
   b. Each employee must ensure that confidential information on computer screens is not visible to unauthorized persons. This can be accomplished by clearing information from the screen when not actually being used, or minimizing all applications when away from the work space or when approached by an unauthorized person.
   c. Confidential information will not be e-mailed or faxed.
   d. When an employee leaves the OPI, the Personnel Office notifies the Information Technology Services Division to immediately terminate the employee's access. Interim access to critical information is the responsibility of the Supervisor.

2. Security of confidential information on paper
   a. Envelopes marked as containing "confidential information" may only be opened by the recipient or their administrator;
   b. Confidential information should only be exposed while the employee is working on the document. All other paper forms of confidential information should be covered in file folder or placed face down on the desktop when not in use (such as break or lunch);
   c. When the employee is away from the desk for an extended period of time (such as being away for two or more hours) all confidential information must be contained in a locked filing cabinet;
   d. When confidential information is no longer needed, it must be shredded; and

3. Security of confidential information in other media, such as verbal communication.
   a. Verbal conversations regarding confidential information must only be to authorized personnel and should use as little identifying information as possible. For example, a conversation could identify the student with a number rather than a name. In all cases, the conversation must be limited to the minimum information necessary to accomplish the purpose of the communication;
   b. Verbal conversations about confidential information should be conducted in a manner and setting that minimizes the amount of the conversation that can be overheard by other individuals;

If you have questions concerning this matter, contact your supervisor or Human Resources at 444-3161.

My signature indicates that I have read and understand the guidelines regarding confidentiality and I agree to abide by these guidelines.

_____
(Printed Name)

_____ _____
(Signature) (Date)

EXHIBIT 3
DATE 2/3/09
HB 2

MONTANA OFFICE OF PUBLIC INSTRUCTION

STUDENT RECORDS CONFIDENTIALITY POLICY

Adopted February 1, 2008

Last Updated July 17, 2008

Linda McCulloch, Superintendent
Montana Office of Public Instruction
PO Box 202501
Helena, Montana 59620-2501
Toll Free: 1-888-231-9393, Local: 406-444-3095
www.opi.mt.gov

Montana Office of Public Instruction
Student Records Confidentiality Policy

Contents:

Student Records Confidentiality Policy
Montana Office of Public Instruction

I. PURPOSE

The purpose of this policy is to establish procedures and responsibilities governing the access, use and dissemination of confidential, sensitive and/or restricted student information by the Office of Public Instruction (OPI).

The collection of individual student information in AIM will replace previous collections of aggregated data from the following data systems:

- ADC (Annual Data Collection)
- MAEFAIRS (Montana Automated Education Finance and Information Reporting System)
- Carl Perkins Accountability
- Special Education Child Count

II. AUTHORIZATION

Individual student education records are submitted to the OPI for all students enrolled in K-12 public schools. The authority to require the submission of data is found in MCA 20-9-309 (2) (g) (See Exhibit 1). The initial appropriation for a K-12 Educational Data System was made in House Bill 2 from the 2005 legislative session. House Bill 2 (L. 2005) can be found at http://data.opi.mt.gov/bills/2005/billhtml/HB0002.htm.

The collection of student data will help facilitate the following:

- promote efficiencies (reduce reporting burden);
- build on existing technologies;
- provide a common basis of data reporting; and
- promote accountability needed to receive state funding.

III. SCOPE OF POLICY

These policies and procedures apply to all contractors and employees of the OPI and to all other entities requesting access to confidential, sensitive, or restricted student information.

Related policies, laws, operating procedures and other documents which contain directives that apply to agency confidential, sensitive and restricted enterprise information include:

- Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99 located at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html (See Exhibit 2.)
- State of Montana Policies located at http://itsd.mt.gov/policy/itpolicy.asp
    - ENT-SEC-041 Transmission Policy
    - ENT-SEC-130 Remote Access for Employees and Contractors
    - ENT-SEC-022 Network Server Security
    - ENT-INT-030 Internet Privacy and Security
    - ENT-SEC-081 User Responsibility
- Release of Information to the Public under the Public Information Act. MCA 2-6-102

- Montana School Accreditation Standards and Procedures Manual located at http://www.opi.mt.gov/pdf/accred/05accredmanual.pdf
- Destruction of Local Government Records, MCA 2-6-405 (d)
- Montana Secretary of State, Local Government Retention and Disposition Schedule located at http://sos.mt.gov/RMB/Local_Forms.asp#Local.
- OPI Records Management Policy
- Public Law 103-448, Section 9 and 108

IV. DEFINITIONS

Personally Identifiable Student Information
FERPA regulations defining *personally identifiable student information* include the following:

- The student's name;
- The name of the student's parent or other family member;
- The address of the student or student's family;
- A personal identifier such as social security number or student number;
- A list of personal characteristics that would make the student's identity easily traceable; or
- Other information that would make the student's identity easily traceable.

The above information cannot be disclosed without compliance with the requirements of FERPA.

Education Record
Education records are defined in FERPA as those records, files, documents, and other materials that contain information directly related to a student and are maintained by an education agency or institution or by a person acting for such agency or institution. 20 U.S.C. §1232g(a)(4). An education record is considered confidential because it contains personally identifiable information about a student.

All information submitted will be considered an education record and, therefore, is protected by Family Educational Rights and Privacy Act (FERPA, Exhibit 2). This federal law limits who can see an education record.

Student Records and Confidentiality Guidelines are outlined in Appendix C-1 of the Montana School Accreditation Standards and Procedures Manual located at http://www.opi.mt.gov/pdf/accred/05accredmanual.pdf.

Student Data Elements
Student data elements are individual pieces of data collected and stored by the OPI in a student's education record. The student data elements collected in the OPI's student information system are defined in the *AIM Data Dictionary* located at www.opi.mt.gov/pub/aim/DTA%20Dictionary.

Directory Information
FERPA allows school systems to establish a policy that designates some types of information as *directory information.* Directory information pertains to the portion of the education record that would not generally be considered harmful or an invasion of privacy if disclosed. Local education agency definitions of directory information may vary, but they generally include a student's name, address, and telephone number, and other

information typically found in school yearbooks or athletic programs. The FERPA regulations define *directory information* under § 99.3 of the regulations and set forth the requirements for implementing a directory information policy under § 99.37 of FERPA (Exhibit 2). Generally, *directory information* may be disclosed by a school to any party, provided the requirements of FERPA are followed. The OPI does not track the variation among local education agencies of their definitions of directory information. Additionally, the OPI is not informed which parents throughout Montana have refused to consent to disclosures of any personally identifiable information (some of which can be the same as directory information). Therefore, the OPI does not release directory information to any source.

Disclosure
Disclosure is to permit access to or the release, transfer, or other communication of education records, or the personally identifiable information contained in those records, to any party, by any means, including oral, written, or electronic means as defined in Appendix C of the Montana School Accreditation Standards and Procedures Manual.

V. STUDENT LOCATOR INFORMATION

Student-centered data collection systems such as AIM require the ability to assign a unique student identifier. An identifier is a computer-generated random number with no embedded meaning and is assigned to an individual student. This unique identifier is sometimes referred to as a "State ID." For the identifier to be unique, each student cannot have more than one identifier and each identifier cannot be associated with more than one student.

To ensure that each student has only one state identifier and that a single identifier is not assigned to more than one student, it is necessary for school personnel to review and locate whether a student has already been assigned a unique identifier before assigning a new identifier to any newly enrolled student. The process of reviewing and locating whether the student has already been assigned a unique identifier requires school personnel to access student locator information. Locator information includes:

- Student name
- Date of birth
- State ID
- Gender

The majority of locator information is confidential. Authorized school personnel have access to confidential locator information provided they have a reason for gaining access, such as the responsibility to assign unique student identifiers, or to determine if a student has already received a State ID, as may be the case when a student transfers from one school to another. All authorized school personnel who have access to confidential information must be familiar with policies and procedures to ensure confidentiality.

VI. PROGRAM PARTICIPATION INFORMATION

Program participation information identifies areas of program concentration and educational services provided to a student while enrolled in the school. Examples of the fields in this collection include students' status in relation to Title I, Free/Reduced Meal, LEP, Homeless, and Special Education. A complete list of fields can be found in the File Specifications document on the OPI AIM web site at http://www.opi.mt.gov/pub/AIM/File Specifications/. This information is part of the student's education record. Reporting of this information is subject to the OPI's policy for cell suppression.

VII. CELL SUPPRESSION POLICY

No cells of data that contain fewer than 10 students in a group will be publicly reported or released and must be suppressed to protect the identity of the student. The exceptions to this policy are enrollment, grade level, and gender, which are reportable down to one. The OPI will suppress data in the form of percentages when the percents are 0 or 100 for any student demographic categories with the exception of reports required under the State Accountability Workbook under NCLB. At the present time, this includes the following indicators: graduation, attendance, participation rates, and proficiency levels.

Any given numeric or non-numeric characteristic, variable values, or data element shared by fewer than 10 students in individual or aggregate (e.g., school, district, state) data sets or reports may contain potentially confidential student information. Even non-confidential student information may be confidential when combined with other data elements.

The OPI will report student counts to the U.S Department of Education and other federal agencies as required by federal laws and regulations governing education grant programs. The OPI will not suppress data reported to federal agencies. These federal agencies are subject to FERPA policy and regulations regarding the disclosure of confidential student information.

VIII. DISCLOSURE OF STUDENT INFORMATION

Part of the education record includes personal information about a student that can be made public according to this policy. The OPI may disclose, without consent, student information in aggregate form which is not easily traceable to a student. This information will follow the guidelines indicated in Section IX of this policy titled Obtaining Access to Student Information.

The OPI will disclose education records, without consent, to the parties listed immediately below under the following conditions:

- other schools when a student is transferring in order to facilitate school enrollment;
- specified officials for audit or evaluation purposes;
- organizations authorized by a school to conduct certain studies for or on behalf of the school; and
- appropriate officials in cases of health and safety emergencies.

The OPI recognizes school districts have developed their own policies to address FERPA (34 CFR § 99.31) compliance. In general, information about each request for records access and each disclosure of information

from an education record must be maintained as part of the record until the school or agency destroys the education record in accordance with the Montana Local Government Retention and Disposition Schedule, which can be found at http://sos.mt.gov/RMB/Local_Forms.asp#Local. The OPI AIM Records Retention Schedule can be found at http://www.opi.mt.gov/pub/AIM/AIM%20Policies.

IX. OBTAINING ACCESS TO STUDENT INFORMATION

This section describes the conditions under which the OPI will release confidential student information. Confidentiality refers to a person's obligation not to disclose or transmit information to unauthorized parties.

A. Access to Confidential Student Information

Access to confidential information carries with it the responsibility to protect the data. Access to confidential student information shall be granted only to personnel who are authorized by the OPI on a need-to-know basis in the performance of their duties.

An OPI Employee AIM and E-Grant Access Request Form (Exhibit 3) or an Affidavit of Non-Release of Data (Exhibit 4) must be signed by the requesting entity before any data will be released. Authorization must be evaluated annually to ensure access to the data is still required.

Intentional violations of this policy by an OPI employee may result in formal disciplinary action, up to and including termination, denial of access to sensitive data, and revocation of network access privileges.

Violation of this policy by agents of the OPI, other entities, or researchers inappropriately releasing data from an education record, whether through negligence or intent, will be subject to potentially permanent loss of access to education records. The OPI may utilize all legal remedies to recover any financial loss to the State which occurs due to negligent or intentional acts which constitute a violation of this policy. Any agents, other entities, or researchers who violate this policy, whether through negligence or intent, shall pay for the defense of all claims asserted against the State as a result of such violation.

The entities to which information may be released and the conditions of the release are listed for each entity below.

1) **OPI Staff** – The OPI staff who have a need to access confidential information in AIM must complete and submit an OPI Employee AIM Access Request Form (Exhibit 3) and the OPI Confidentiality Agreement (Exhibit 8) to the OPI Information Technology Services Division. The division administrator of the person requesting access to confidential information must sign the form which indicates the person needs access to this information in the performance of his or her assigned duties and responsibilities. The division administrator will ensure that the appropriate safeguards are instituted to protect the confidentiality of student information and that the staff person has received AIM training. The OPI staff may not access agency information for personal purposes (for example, research for a dissertation). Data will be destroyed in accordance with OPI's record retention policy.

Those staff who do not need access to AIM but who use confidential information concerning students or school districts in the course of their job duties must sign Exhibit 8 (OPI Confidentiality Agreement).

2) **Agent of the OPI** – An agent of the OPI is an entity that contracts with the OPI or with the U.S. Department of Education (DOE) and has written authorization from the DOE to analyze confidential data, or to provide some other service involving confidential data. When an agent contracts with another entity to provide a service involving confidential data, these entities are considered agents for data purposes. The OPI staff responsible for contracting with an entity to analyze confidential data or to provide some other service involving confidential data must ensure that the terms of the contract comply with the same conditions applicable to the OPI staff and that an Affidavit of Non-Release of Data (Exhibit 4) has been signed by the organization. A copy of the Affidavit of Non-Release of Data will be kept on file at the OPI, Information Technology Services Division. The agency staff person responsible for releasing the data must ensure that the Affidavit of Non-Release of Data has been signed prior to the data being released.

3) **Other Entities** – All other entities will be denied access to confidential information unless the entity is using the data to develop, validate, or administer predictive tests or improve instruction as defined in FERPA 34 C.F.R. § 99.31(a)(6). Authorized representatives of the Comptroller General of the United States, the Secretary of the U.S. Department of Education, or state and local educational authorities will be provided access to the data provided the disclosure is in the course of an audit, evaluation, compliance, or enforcement proceeding as defined in FERPA 34 C.F.R. §§ 99.31(a)(3), 99.35. The information will be protected to shield personal identification of students by others and the information will be destroyed when no longer needed.

4) **Researchers** - Researchers who are not an agent of the OPI or who are not employed or contracted by the agency or school may be authorized to conduct data processing or research and evaluation studies through contractual arrangements. Requests from researchers will be handled on a case-by-case basis after the request has been approved by the Data Privacy and Security Committee at the OPI. The Data Privacy and Security Committee members include the Measurement and Accountability Division Administrator, Chief of Staff, and Chief Legal Counsel at the OPI.

Items taken into consideration before releasing student data include:

- Perceived benefits of the research;
- Degree to which the research question cannot be answered without the confidential data;
- Potential invasion of student's privacy;
- Experience and reputation of the requester;
- Capacity of the requester to keep the data secure; and
- Availability of the OPI staff to fulfill the data request for the research project and monitor the process of the release and the research activities.

Such data will not be released unless the data are requested by an individual or organization who either (a) has developed a Research Proposal (Exhibit 6) which has been approved by the OPI Data Privacy and Security Committee and has completed the Research Project Confidentiality Agreement (Exhibit 7) or (b) has completed an Affidavit of Non-Release of Data (Exhibit 4). Once approval has been given to the researcher, the data will be posted to a secure file transfer protocol site which may then be downloaded.

In general, the release of data to researchers outside the agency is considered a loan of data (i.e., recipients do not have ownership of the data). Any personally identifiable student information shared with researchers must be destroyed when the data is no longer needed for the purposes for which it was requested.

Any requests for confidential student information from entities other than the OPI staff and its agents that do not meet the conditions of Section IX of this policy shall be directed to the district from which that information originated.

B. Procedures for Protecting Student Data

All agency employees, agents of the OPI, researchers, and other entities with direct access to confidential student information are responsible for protecting the data via the following procedures:

- Prevent disclosure of data by protecting visibility of reports and computer monitor when displaying confidential information.
- Workstations must be locked or shutdown when unattended.
- If reports containing any confidential student information are used in meetings or presentations, or presented to anyone without authorized access to the information, the agency employee or contractor must change the data to guarantee anonymity and omit or mask counts less than ten. One possible method for eliminating small counts is to reduce the number of variables used when selecting records (for example, by eliminating gender, the count may double).
- When no longer needed, paper reports must be shredded and electronic files must be destroyed in accordance with the Montana Secretary of State, Local Government Retention and Disposition Schedule.
- Confidential student information will not be faxed.
- Reports, CDs, and diskettes containing confidential student information must be stamped or otherwise marked as confidential prior to being released outside the agency. The envelope containing the information must also indicate that the contents are confidential.
- Confidential student information must be sent using encrypted email or by using the file transfer process set up in E-Pass. Instruction for using E-Pass can be found at http://opi.mt.gov/ITProjects/epass.html. Questions and concerns about transferring confidential data may be addressed to the OPI Network Services Bureau.

X. TRAINING NEEDS

All OPI staff and other entities requesting access to confidential student information shall be made aware of the AIM Student Records Confidentiality Policy and will receive subsequent information through newsletter articles, e-mail messages, and/or training classes.

XI. RESPONSIBILITY FOR PROCESS

The Information Technology Services and Measurement and Accountability Division at the OPI are primarily responsible for releasing AIM data once the appropriate form (Exhibit 3, 4, or 7) has been signed and approval has been granted by the Data Privacy and Security Committee.

The OPI Security Officer will file copies of all signed and approved file access request forms and confidentiality agreements (Exhibits 3, 4, 6, 7, 8) with the applicable data request. Any rights that need to be assigned to staff, agents of the OPI, or other entities will be assigned by the OPI Information Technology Services Division.

The OPI Measurement and Accountability Division staff are primarily responsible for releasing AIM data once the appropriate form (Exhibit 3, 4 or 7) has been signed and, for researchers, approval has been granted by the Data Privacy and Security Committee (Exhibit 6). The OPI Measurement and Accountability Division staff shall maintain a record which indicates the name of any individual or organization external to the OPI that requests data. The record of access shall also indicate the interest such individual or organization had in obtaining the information, the fields of data requested, and the date the requested data were disclosed. Once approval has been granted, the OPI Security Officer will process the security authorization and set up access to the records in compliance with FERPA guidelines.

XII. PROCESS FOR HANDLING INFORMATION REQUESTS FROM RESEARCHERS

Over the past several years, the OPI has received a growing number of information and data requests from researchers. Traditionally, these requests were handled on a case-by-case basis. However, as the number of such requests has grown, it has become necessary for the OPI to standardize the request approval process in order to handle these requests in a fair and timely manner. A description of the process follows.

A. External data requests for specific information will be honored only if one of the following is true:

1) The material requested has already been published or collected and can easily be put into a distribution format that protects confidential information. In these cases, information can be provided without a review by the OPI Data Privacy and Security Committee.

2) The requestor completes the process for conducting research with OPI data and has his/her proposal approved by the OPI Data Privacy and Security Committee. (See Exhibits 5 and 6.) Directions for an application to conduct research with student level data collected by the OPI are included in Exhibit 5.

B. Proposals submitted to the OPI Data Privacy and Security Committee will be subject to the following:

1) Before review by the OPI Data Privacy and Security Committee, proposals may be forwarded to appropriate staff within the OPI for their comments and recommendations. Information provided by the OPI staff will be considered in the proposal review.

2) Research proposals that fall under the OPI's primary mission statement will receive first priority.

3) The OPI staff resources may limit the number of requests that can be honored during a fiscal year. Thus, some worthy studies that receive approval may need to be postponed until OPI resources are available.

4) A charge may be associated with a data request/research proposal, including those approved by the OPI Data Privacy and Security Committee. The charge for already published documents will be determined by printing and mailing costs. The charge for conducting data selection/analysis tasks associated with a research proposal will vary but will not exceed $50 per hour. Cost estimates, if any, will be provided to the researcher upon request.

5) A conference will be held, by phone or in person, with researchers whose proposals have been accepted. During the conference, members of the OPI Data Privacy and Security Committee and the researcher(s) will come to an agreement on objectives, end products, timelines, areas of responsibility, data security arrangements, authorship credit, and costs. A written statement outlining the terms of the agreement will be signed by the researcher and a designee of the OPI Data Privacy and Security Committee.

6) A Research Project Confidentiality Agreement must be signed by each researcher once the OPI Data Privacy and Security Committee approves the research request for data. (See Exhibit 7.)

7) The OPI Data Privacy and Security Committee will meet as needed to consider proposals.

8) Researchers will provide a copy of products resulting from the research (e.g., publication, report, book) to the OPI Data Privacy and Security Committee.

C. Documentation of all research requests will be maintained.

1) The OPI staff will track each research project and data request.

2) Files sent and technical assistance given to researchers will be included in the data request tracking documentation.

3) The OPI staff will attach a copy of the end result of a research project (publication, report, book) or a link to the material to the data request tracking documentation.

XIII. ENFORCEMENT

The Family Policy Compliance Office of the U.S. Department of Education is responsible for enforcement regarding concerns of breach of confidentiality or violations of FERPA and can be reached by calling (202) 260-3887 or at the following address:
US Department of Education
600 Independent Avenue, SW
Washington, DC 20202-4605

XIV. EXHIBIT 1
Statutory Authorization to Collect Student Data

The authority to require the submission of data is found in MCA 20-9-309 (2) (g). The initial appropriation for a K-12 Educational Data System was made in House Bill 2 from the 2005 legislative session. The complete text of House Bill 2 can be found at http://data.opi.mt.gov/bills/2005/billhtml/HB0002.htm.

MCA 20-9-309. Basic system of free quality public elementary and secondary schools defined -- identifying educationally relevant factors -- establishment of funding formula and budgetary structure -- legislative review. (1) Pursuant to Article X, section 1, of the Montana constitution, the legislature is required to provide a basic system of free quality public elementary and secondary schools throughout the state of Montana that will guarantee equality of educational opportunity to all.

(2) As used in this section, a "basic system of free quality public elementary and secondary schools" means:

(a) the educational program specified by the accreditation standards provided for in 20-7-111, which represent the minimum standards upon which a basic system of free quality public elementary and secondary schools is built;

(b) educational programs to provide for students with special needs, such as:

(i) a child with a disability, as defined in 20-7-401;

(ii) an at-risk student;

(iii) a student with limited English proficiency;

(iv) a child who is qualified for services under 29 U.S.C. 794; and

(v) gifted and talented children, as defined in 20-7-901;

(c) educational programs to implement the provisions of Article X, section 1(2), of the Montana constitution and Title 20, chapter 1, part 5, through development of curricula designed to integrate the distinct and unique cultural heritage of American Indians into the curricula, with particular emphasis on Montana Indians;

(d) qualified and effective teachers or administrators and qualified staff to implement the programs in subsections (2)(a) through (2)(c);

(e) facilities and distance learning technologies associated with meeting the accreditation standards;

(f) transportation of students pursuant to Title 20, chapter 10;

(g) *a procedure to assess and track student achievement in the programs established pursuant to subsections (2)(a) through (2)(c)*; and

(h) preservation of local control of schools in each district vested in a board of trustees pursuant to Article X, section 8, of the Montana constitution.

(3) In developing a mechanism to fund the basic system of free quality public elementary and secondary schools and in making adjustments to the funding formula, the legislature shall, at a minimum, consider the following educationally relevant factors:

(a) the number of students in a district;

(b) the needs of isolated schools with low population density;

(c) the needs of urban schools with high population density;

(d) the needs of students with special needs, such as a child with a disability, an at-risk student, a student with limited English proficiency, a child who is qualified for services under 29 U.S.C. 794, and gifted and talented children;

(e) the needs of American Indian students; and

(f) the ability of school districts to attract and retain qualified educators and other personnel.

(4) By July 1, 2007, the legislature shall:

(a) determine the costs of providing the basic system of free quality public elementary and secondary

schools;

(b) establish a funding formula that:

(i) is based on the definition of a basic system of free quality public elementary and secondary schools and reflects the costs associated with providing that system as determined in subsection (4)(a);

(ii) allows the legislature to adjust the funding formula based on the educationally relevant factors identified in this section;

(iii) is self-executing and includes a mechanism for annual inflationary adjustments;

(iv) is based on state laws;

(v) is based on federal education laws consistent with Montana's constitution and laws; and

(vi) distributes to school districts in an equitable manner the state's share of the costs of the basic system of free quality public elementary and secondary schools; and

(c) consolidate the budgetary fund structure to create the number and types of funds necessary to provide school districts with the greatest budgetary flexibility while ensuring accountability and efficiency.

(5) At least every 10 years following April 7, 2005, the legislature shall:

(a) authorize a study to reassess the educational needs and costs related to the basic system of free quality public elementary and secondary schools; and

(b) if necessary, incorporate the results of those assessments into the state's funding formula.

History: En. Sec. 2, Ch. 208, L. 2005.

XV. EXHIBIT 2
An Overview of the Family Educational Rights and Privacy Act (FERPA)

Student education records are official and confidential documents protected by one of the nation's strongest privacy protection laws, the Family Educational Rights and Privacy Act (FERPA). FERPA, also known as the Buckley Amendment, defines education records as all records that schools or education agencies maintain about students.

FERPA gives parents (as well as students in postsecondary schools) the right to review and confirm the accuracy of education records. This and other United States "privacy" laws ensure that information about citizens collected by schools and government agencies can be released only for specific and legally defined purposes. Since enacting FERPA in 1974, Congress has strengthened privacy safeguards of education records through this law, refining and clarifying family rights and agency responsibilities to protect those rights.

FERPA's legal statute citation can be found in the U.S. Code (20 USC 1232g), which incorporates all amendments to FERPA. FERPA regulations are found in the Federal Register (34 CFR Part 99). FERPA's 1994 amendments are found in Public Law (P.L.) 103-382.

FERPA Protects Privacy

FERPA applies to public schools and state or local education agencies that receive Federal education funds, and it protects both paper and computerized records. In addition to the Federal laws that restrict disclosure of information from student records, most states also have privacy protection laws that reinforce FERPA. State laws can supplement FERPA, but compliance with FERPA is necessary if schools are to continue to be eligible to receive Federal education funds.

FERPA requires schools and local education agencies to annually notify parents of their rights under FERPA. The notice must effectively inform parents with disabilities or who have a primary home language other than English. The annual notice pertaining to FERPA rights must explain that parents may inspect and review records and, if they believe the records to be inaccurate, they may seek to amend them. Parents also have the right to consent to disclosures of personally identifiable information in the record, except under authorized circumstances.

FERPA gives both parents, custodial and non-custodial, equal access to student information unless the school has evidence of a court order or state law revoking these rights. When students reach the age of 18, or when they become students at postsecondary education institutions, they become "eligible students' and rights under FERPA transfer to them. However, parents retain access to student records of children who are their dependents for tax purposes.

FERPA Defines an Education Record

Education records include a range of information about a student that is maintained in schools in any recorded way, such as handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche. Examples are:

- *Date and place of birth, parent(s) and/or guardian addresses, and where parents can be contacted in emergencies;*
- *Grades, test scores, courses taken, academic specializations and activities, and official letters regarding a student's status in school;*
- *Special education records;*
- *Disciplinary records;*
- *Medical and health records, including immunization records, that the school creates or collects and maintains;*
- *Documentation of attendance, schools attended, courses taken, awards conferred, and degrees earned;*
- *Personal information such as student's identification code, social security number, picture, or other information that would make it easy to identify or locate a student.*

Personal notes made by teachers and other school officials that are not shared with others are not considered education records. Additionally, law enforcement records created and maintained by a school or district's law enforcement unit are not education records.

Part of the education record, known as ***directory information***, includes personal information about a student that can be made public according to a school system's student records policy. Directory information may include a student's name, address, and telephone number, and other information typically found in school yearbooks or athletic programs. Other examples are names and pictures of participants in various extracurricular activities or recipients of awards, pictures of students, and height and weight of athletes.

Each year schools must give parents public notice of the types of information designated as directory information. By a specified time after parents are notified of their review rights, parents may ask to remove all or part of the information on their child that they do not wish to be available to the public without their consent.

FERPA Guarantees Parent Review and Appeal

If, upon review, parents find an education record is inaccurate or misleading, they may request changes or corrections, and schools and education agencies must respond promptly to these requests.

Requests should be made in writing, according to an agency's annual notice of procedures for exercising rights to amend records. Within a reasonable time period, the school or agency must decide if the request to change a record is consistent with its own assessment of the accuracy of the record. If a parent's request is denied, he or she must be offered the opportunity for a hearing. If the disagreement with the record continues after the hearing, the parent may insert an explanation of the objection in the record. FERPA's provisions do not apply to grades and educational decisions about children that school personnel make.

While parents have a right to review records, schools are not required by Federal law to provide copies of information, unless providing copies would be the only way of giving parents access. Schools may charge a reasonable fee for obtaining records, and they may not destroy records if a request for access is pending.

FERPA Restricts Disclosure of Student Records

Local education agencies and schools may release information from students' education records with the prior written consent of parents, under limited conditions specified by law, or as stated in local agencies' student records policies. The same rules restricting disclosures apply to records maintained by third parties acting on behalf of schools, such as state and local education agencies, intermediate administrative units, researchers, psychologists, or medical practitioners who work for or are under contract to schools.

If an agency or school district has a policy of disclosing records, it must specify the criteria for determining school officials within an agency, including teachers, who have a legitimate educational interest. Generally, school officials have legitimate educational interest if they need to review an education record to fulfill their professional responsibilities.

Teachers and school officials who work with the students and schools to which students apply for entrance may also have access to education records without prior consent of the parent. In addition, information from students' records may be released to state and local education officials to conduct audits or to review records in compliance with Federal laws. Schools may also disclose information from education records without the consent of parents in response to subpoenas or court orders. A school official must make a reasonable effort to notify the parent before complying with the subpoena unless the subpoena is issued to enforce a law and specifies not to notify the parent. In emergencies, school officials can provide information from education records to protect the health or safety of the student or others.

There are cases when schools or school systems decide it is in the public interests to participate in policy evaluations or research studies. If student records are to be released for these purposes, the school or school system must obtain prior consent of the parent. Signed and dated written consent must:

- *Specify the records that will be released;*
- *State the reason for releasing the records;*
- *Identify the groups or individuals who will receive the records.*

In general, information about each request for records access and each disclosure of information from an education record must be maintained as part of the record until the school or agency destroys the education record. Outside parties receiving records must receive a written explanation of the restrictions on the re-release of information.

Additional FERPA Provisions

In 1994, the Improving America's School Act amended several components of FERPA, tightening privacy assurances for students and families. The amendments apply to the following key areas:

- *Parents have the right to review the education records of their children maintained by the state education agencies;*
- *Any third party that inappropriately re-releases personally identifiable information from an education record cannot have access to education records for five years;*
- *Information about disciplinary actions taken against students may be shared, without prior consent of the parent, with officials in other education institutions;*
- *Schools may release records in compliance with certain law enforcement judicial orders and subpoenas without notifying parents.*

Questions? Call the Local School System, State Education Agency, or the Federal Family Policy Compliance Office.

School districts, state education agencies, and the U.S. Department of Education all offer assistance about FERPA. Before contacting Federal officials, however, you can often get a direct and immediate response from your local or state education officials.

The **Family Policy Compliance Office** can be reached at the following address;

U.S. Department of Education
600 Independent Avenue, SW
Washington, DC 20202-4605
(202) 260-3887

XVI. EXHIBIT 3
OPI Employee AIM Access Request

This form will be used to identify each individual who will use AIM. . The completed form is to be sent to the OPI Help Desk who will set up the user security roles. If you have questions regarding this form, please contact the OPI Help Desk at 444-3448.

Name of Individual Requesting Access: *(Please Print)* _____

Division: _____ Bureau: _____

Briefly describe your primary use of the AIM system: _____

_____

_____

TYPE OF ACCESS REQUESTED:

- ☐ **Read** - Read-only rights to specific student information (census, enrollment, & state reporting tools). Rights to view calendars. No read rights to specific special education information or database/system administrator tools.
- ☐ **Read All** - Read-only rights to all student information (census, enrollment & state reporting tools); including read only rights to special education data. Rights to all view calendars.
- ☐ **Ad Hoc Reporting** – Allows user to create, edit, and delete filters. Rights to export data for reports. Rights to create, modify and save a cube.
- ☐ **District Assistance RW**- Allows user to modify specific student information (census, enrollment & state reporting data elements) to assist districts with their data entry and clean up. Rights to all calendars. Rights to view special education status. No rights to view special education data (forms, IEP). No rights to update directory information.
- ☐ **District Assistance RWAD**- Allows user to enter, modify, and delete a student record (census, enrollment & state reporting data elements) to assist districts with their data entry and clean up. Rights to all calendars and all student information (excluding special education data). No rights to update or view special education data. No rights to update directory information.
- ☐ **Directory R** – Allows user to view school and district directory information (System Admin>Resources).
- ☐ **Directory RWA**- Allows user to view, modify and add school and district directory information (System Admin>Resources).
- ☐ **Combine/Delete Records** - Rights to combine duplicate student records and delete enrollments student records. No rights to update directory information.
- ☐ **Migrant** – Allows user to modify student enrollment data, specifically migrant information.
- ☐ **Special Education Read** - Read rights all student information including special education specific data (summary, team members, documents, contact log). Rights to all calendars.
- ☐ **Special Education Monitors RW**– Allows user to modify (or write) specific areas of the Special Education documents including IEP.
- ☐ Other (Describe specific duties): _____

_____

CONFIDENTIALITY/CONSENT STATEMENT: *(To be read and signed by the individual requiring access.)*
I hereby certify that I am entitled to the confidential information to which I am requesting access. I will not release the confidential information to others unless it is for purposes directly connected to the administration of the program for whose purposes it was originally provided. Intentional violations of the OPI Student Records Confidentiality Policy may result in formal disciplinary action, up to and including termination, denial of access to sensitive data, and revocation of network access privileges. I have read and signed the OPI Network Acceptable Use Policy, the OPI Student Records Confidentiality Policy, and the State of Montana's Computer Use Policies and I agree to comply with all terms and conditions.

Employee Signature: _____ Date: _____

Division Administrator Signature: _____ Date: _____

This section to be completed by the OPI security officer

Signature of Security Officer: _____ Date: _____

Access Approved: ☐ Access Denied: ☐ Logon ID: _____

XVII. EXHIBIT 4
Affidavit of Non-Release of Data for Agents of OPI or Other Entities

This form will be used to identify an agent of OPI or other entity who requests access to confidential student information. The completed form is to be sent to the OPI Help Desk who will forward it to the OPI Data Privacy and Security Committee for review and approval. Once approved, the OPI Help Desk will set up the user security roles. If you have questions regarding this form, please contact the OPI Help Desk at 444-3448.

I, _____, do solemnly swear that when given access to the student information data provided by the OPI, I shall only 1) use, reveal, or in any other manner disclose any personally identifiable information furnished, acquired, retrieved, or assembled by me or others, or 2) make any release or publication by which an individual could be identified to authorized staff at the OPI and authorized school district representatives in order to: (check all that apply)

☐ Audit or evaluate

☐ Comply with an enforcement proceeding

☐ Improve instruction

☐ Develop, validate, or administer predictive tests

☐ Provide training and system support

☐ Other (please describe) _____

I shall not permit anyone other than the individuals authorized by _____ (name of the agency or school) to examine the individual records.

The re-release of such student information in any other circumstances is prohibited by the Family Educational Rights and Privacy Act of 1974.

Please provide a detailed description of how the data will be kept secure, including computer security, physical handling, and storage and transportation of data.

_____

I understand if, through my negligent or intentional acts, I violate this policy by inappropriately releasing data from an education record, I will be subject to potentially permanent loss of access to education records. Additionally, I understand and agree the OPI may utilize all legal remedies to recover for any financial loss to the State which occurs due to my negligent or intentional acts which constitute a violation of this policy. I further agree to pay for the defense of all claims asserted against the State as a result of my negligent or intentional acts which constitute a violation of this policy.

Signature: _____

Name: _____ Title: _____

Organization: _____ Date: _____

Notary Public and Seal: _____

This section to be completed by the OPI staff:
LOA or Contract #

Access Approved ☐ _____ **Access Denied** ☐ _____
Effective Dates of Contract: _____

Signature of Security Officer: _____ **Date:** _____

XIX. EXHIBIT 5
Directions for Application to Conduct Research with Student Level Data Collected by the OPI

Student level data will be released to researchers who complete the Research Proposal Application (Exhibit 6) after the proposal has been approved by the OPI Data Privacy and Security Committee and the Research Project Confidentiality Agreement (Exhibit 7) has been signed by the responsible parties. Researchers who are interested in such an arrangement should comply with the following directions. Those agencies under contract with the OPI must complete and sign the Affidavit of Non-Release of Data for Agents of the OPI or Other Entities (Exhibit 4).

1. Researcher must complete the Research Proposal Application (Exhibit 6) and submit the form to the OPI Measurement and Accountability Division, Office of Public Instruction, PO Box 202501, Helena, Montana 59620-2501.

2. Research proposals received will be reviewed by the OPI Data Privacy and Security Committee. As necessary, the OPI legal staff and program staff from the department most closely connected to the research topic may be included in the review process. Researchers will be informed of the committee's decision about acceptance/rejection of the proposal in as timely a manner as possible.

3. Either at the time of the submission of the documents referred to in item 1, or upon having a research project accepted, the researcher must complete the Research Project Confidentiality Agreement (Exhibit 7) and send it to the OPI Measurement and Accountability Division.

4. Once a proposal is accepted, researchers and the appointed OPI liaison will confer for the purpose of developing an agreement related to objectives, end products, timelines, areas of responsibility, data security arrangements, authorship credit, and costs. This agreement must be signed by the Researcher and approved by the OPI liaison.

5. Once an agreement has been signed, access to data will be granted.

6. Questions about directions or procedures for research may be addressed to the Office of Public Instruction, Measurement and Accountability Division.

XVIII. EXHIBIT 6
Research Proposal Application

This form will be used to identify the researcher who requests access to confidential student information. The completed form should be submitted to the OPI Data Privacy and Security Committee, Office of Public Instruction, PO Box 20501, Helena, MT 59620-2501.

Title of Proposed Research Project:	
Research Individual or Organization Name:	
Address:	
Name of Primary Researcher:	
Title:	
Phone:	Email:

Provide a description of the research to be performed, including the following:

1) the research question(s) to be addressed;
2) potential improvements or benefits to Montana education of answering the questions;
3) the organization sponsoring the research;
4) research timeline;
5) the specific data items that will be requested from the Montana Office of Public Instruction (OPI);
6) other data that will be collected for the research and from whom;
7) how the data will be used and analyzed;[1]
8) how the analysis will be reported and to whom;
9) the names and titles of the professional and support staff who will conduct the research and analysis;[2]
10) the estimated time the data from the OPI will be needed; and
11) a detailed description of how the data will be kept secure, including computer security, physical handling and storage of data, and transportation of data.

This section to be completed by the OPI Data Privacy and Security Committee
Signature: _____ Date: _____

Access Approved: ☐ Access Denied: ☐

[1] Data must only be used for purposes associated with the data collection and analysis specified in this Research Proposal.
[2] Attach research staff VITA.

XX. EXHIBIT 7
Research Project Confidentiality Agreement

The Montana Office of Public Instruction (OPI) has collected certain data that contain confidential personally-identifiable information; the OPI requires this confidentiality to be protected.

The OPI is willing to make these data available for research and analysis purposes to improve instruction in public elementary and secondary schools, but only if the data are used and protected in accordance with the terms and conditions stated in this Agreement.

_____

(Insert typed name and address of Research Organization) (Researcher) and the OPI agree as follows:

I. INFORMATION SUBJECT TO THIS AGREEMENT

A. All data containing personally-identifiable information collected by or on behalf of the OPI and provided to the Researcher and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by the OPI with other data, are subject to this Agreement and are referred to herein as the "subject data." The subject data under this Agreement may be stated or provided in various forms, including, but not limited, to written or printed documents, computer tapes, diskettes, CD-ROMs, hard copy, or encrypted files.

B. The Researcher may use the subject data only for the purposes stated in the Research Proposal Application attached hereto and made a part of this Agreement (marked as Attachment 1), and is subject to the limitations imposed under the provisions of this Agreement.

II. INDIVIDUALS WHO MAY HAVE ACCESS TO SUBJECT DATA

Researcher agrees to limit and restrict access to the subject data to the following three categories of individuals:

1. The Project Leaders who are in charge of the day-to-day operations of the research and who are the research liaisons with the OPI.

2. The Professional/Technical staff in charge of the research under this Agreement.

3. Support staff including secretaries, typists, computer technicians, etc.; however, these individuals shall be allowed access to the subject data only to the extent necessary to support the research.

III. LIMITATIONS ON DISCLOSURE

A. Researcher shall not use or disclose the subject data for any purpose not expressly stated in the Research Proposal Application approved by the OPI unless the Researcher has obtained advance written approval from the OPI.

B. Researcher may publish the results, analysis, or other information developed as a result of any research based on the subject data made available under this Agreement only in summary or aggregate form, ensuring the identities of individuals included in the subject data are not revealed.

IV. ADMINISTRATIVE REQUIREMENTS

A. The research conducted under this Agreement shall be limited to, and consistent with, the purposes stated in the Research Proposal Application.

B. Notice and training on confidentiality and nondisclosure.

1. Researcher shall notify and train each of its employees who will have access to the subject data of the strict confidentiality of such data, and shall require each of those employees to execute an Affidavit of Non-Release of Data for Agents of OPI, Other Entities or Researchers.

2. Researcher shall maintain each executed Affidavit of Non-Release of Data for Agents of OPI, Other Entities or Researchers at its facility, and shall allow inspection of the same by the OPI upon request.

3. Researcher shall promptly notify the OPI in writing when the access to the subject data by any individual is terminated, giving the name of the individual and the date of the termination.

C. Publications made available to the OPI.

1. Researcher shall provide the OPI a copy of each publication containing information based on the subject data or other data product based on the subject data made available through the OPI.

D. Researcher shall notify the OPI immediately in writing upon receipt of any request or demand for disclosure of the subject data.

E. Researcher shall notify the OPI immediately in writing upon discovering any breach, or suspected breach, of security, or of any disclosure of subject data to an unauthorized party or agency.

V. SECURITY REQUIREMENTS

A. Maintenance of, and access to, the subject data.

1. Researcher shall retain the original version of the subject data at a single location and shall not make a copy or extract of the subject data available to anyone except individuals specified in paragraph II.

2. Researcher shall maintain the subject data (whether maintained on a mainframe facility, central server, personal computer, or in print or other medium materials) in an area with access limited to only authorized personnel. Researcher shall not permit removal of any subject data from the limited access area.

3. Researcher shall ensure access to the subject data maintained in computer files or databases is controlled by password protection. Researcher shall maintain all printouts, diskettes, or other physical products containing individually-identifiable information derived from subject data in locked cabinets, file drawers, or other secure locations when not in use.

4. Researcher shall ensure all printouts, tabulations, and reports are edited to prevent any possible disclosure of personally-identifiable subject data.

5. Researcher shall establish procedures to ensure the subject data cannot be extracted from a computer file or database by unauthorized individuals.

B. Retention of subject data.

1. Researcher shall destroy the subject data, including all copies, when the research that is the subject of this Agreement has been completed or this Agreement terminates, whichever occurs first.

VI. TERMINATION OF THIS AGREEMENT

1. This Agreement shall terminate six months from the date it is signed by the OPI. The Agreement, however, may be extended by written agreement of both of the parties.

2. Any violation of the terms and conditions of this Agreement may result in the immediate revocation of this Agreement by the OPI.

   a. The OPI may initiate revocation of this Agreement by written notice to Researcher indicating the factual basis and grounds of revocation.
   b. Upon receipt of the written notice of revocation, the Researcher shall immediately cease all research activity related to the Agreement until the issue is resolved. The Researcher will have three business days to submit a written Response to the OPI indicating why this Agreement should not be revoked.
   c. The OPI Data Privacy and Security Committee shall decide whether to revoke this Agreement based on all the information available to it. The OPI shall provide written notice of its decision to the Researcher within 10 business days after receipt of the Response. These timeframes may extend for good cause.

SIGNATURE PAGE

By signing below, the individual researcher or official of the Research Organization certifies he or she has the authority to bind the Research Organization to the terms of this Agreement and that the Research Organization has the capability to undertake the commitments in this Agreement.

1. Location at which the subject data will be maintained and analyzed.	
2. Signature of the Individual Researcher or Official of the Research Organization	3. Date
4. Type/Print Name of Official	5. E-mail
6. Title	7. Telephone
8. Mailing Address	
9. Signature of the Principal Research Analyst	10. Date
11. Type/Print Name of Principal Research Analyst	12. E-mail
13. Title	14. Telephone
15. Mailing Address	
16. Signature of OPI Research Liaison	17. Date
18. Type/Print Name of OPI Research Liaison	19. E-mail
20. Title	21. Telephone
22. Mailing Address	

XXI. EXHIBIT 8
OPI Confidentiality Agreement

As an employee of the Montana Office of Public Instruction (OPI) you may often come in contact with confidential information concerning students and school districts. Employees are required to maintain confidentiality in all areas and may include written or computerized district data, other written material or verbal conversations.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

FERPA information must be kept confidential.

The OPI is committed to complying with FERPA and other State and Federal laws protecting our districts' privacy.

Violation of the provisions of FERPA can result in civil and criminal penalties for OPI and disciplinary action against the employee, up to and including termination.

Guidelines for maintaining confidentiality:

1. Access only those records you need to perform your duties or as authorized by your supervisor.
2. Provide confidential information only to those persons who are authorized to receive it. Your supervisor can give you direction if you are unsure about who has access to the information.
3. Report any suspected breach of confidentiality to your supervisor as you become aware of it.

OPI Employees must make reasonable efforts to provide for the security of confidential information.

1. Security of electronic information
   a. Employees will be granted access to only the level of information that is required by their job duties.
   b. Each employee must ensure that confidential information on computer screens is not visible to unauthorized persons. This can be accomplished by clearing information from the screen when not actually being used, or minimizing all applications when away from the work space or when approached by an unauthorized person.
   c. Confidential information will not be e-mailed or faxed.

   d. When an employee leaves the OPI, the Personnel Office notifies the Information Technology Services Division to immediately terminate the employee's access. Interim access to critical information is the responsibility of the Supervisor.

2. Security of confidential information on paper
   a. Envelopes marked as containing "confidential information" may only be opened by the recipient or their administrator;
   b. Confidential information should only be exposed while the employee is working on the document. All other paper forms of confidential information should be covered in file folder or placed face down on the desktop when not in use (such as break or lunch);
   c. When the employee is away from the desk for an extended period of time (such as being away for two or more hours) all confidential information must be contained in a locked filing cabinet;
   d. When confidential information is no longer needed, it must be shredded; and

3. Security of confidential information in other media, such as verbal communication.
   a. Verbal conversations regarding confidential information must only be to authorized personnel and should use as little identifying information as possible. For example, a conversation could identify the student with a number rather than a name. In all cases, the conversation must be limited to the minimum information necessary to accomplish the purpose of the communication;
   b. Verbal conversations about confidential information should be conducted in a manner and setting that minimizes the amount of the conversation that can be overheard by other individuals;

If you have questions concerning this matter, contact your supervisor or Human Resources at 444-3161.

My signature indicates that I have read and understand the guidelines regarding confidentiality and I agree to abide by these guidelines.

_____
(Printed Name)

_____ _____
(Signature) (Date)